SURVEY ON DISTRIBUTED DENIAL OF SERVICE ATTACK USING DEEP LEARNING APPROACHES

D. Sathish[1], A. Kavitha*[2]

ABSTRACT

Nowadays, numerous challenges in cyberspace contribute to the emergence of network security issues. The identification of irregularities in traffic data is critical to the detection of hostile activity inside a network, which is necessary for maintaining the integrity of current Cyber-Physical Systems (CPS) as well as network security. One of the most prevalent and successful types of attacks that aims to prevent or impair the service delivery of its victim(s) is the distributed denial-of-service (DDoS) attack. For non-distributed attacks, the attack detection systems identify a source node with a high volume of packet transmission. DDoS attacks are challenging to identify or stop;thus, many academics have recently concentrated on them. The detection procedure is prolonged by certain factors, including assaults with low traffic rates, losing the durations of successive anomalies, and having a high number of analysis samples. This paper offers a comprehensive taxonomy of DDoS attacks, provides an overview of high-speed network accuracy assessment parameters, and categories detection approaches. In addition, a qualitative study of the literature is conducted to examine the parameters derived from the taxonomy of irregular traffic pattern identification offered. Suggested study areas emphasize the problems and difficulties associated with DDoS attacks on networks, and help researchers discover and build the best possible solution.

Keywords: Distributed Denial of Service (DDoS) attack; Deep learning; Computer Network Security;

I. INTRODUCTION

Today's corporate environment is characterized by a blend of local and global dynamics. While this integration brings numerous benefits, it also elevates your risk profile, particularly in terms of cybersecurity threats. To proactively address, identify, and mitigate these network security challenges, it's essential for your management and IT team to have a comprehensive understanding of the potential attack vectors [1]. The goal of computer network security systems is to defend an organization from network intrusions. The DDoS attack was one of the most prevalent strikes in recent years. A distributed denial-of-service (DDoS) attack is an intentional effort to disrupt the normal operation of a network, service, or website by inundating it with internet traffic. These attacks are orchestrated using a network of remotely controlled computers called a "botnet," which inundates the target system with an overwhelming volume of traffic, preventing legitimate users from accessing it [2]. An example of such an attack is the 2.3 Tbps DDoS incident that targeted Amazon Web Services (AWS) in February 2020 [3]. Google recently disclosed that during June 2022's peak hour, 46 million queries per second were made on one of its cloud clients[4]. DDoS attacks reached a record high in Q4 2021, and the number is continuing to rise, according to Kaspersky Lab[5].A DDoS attack is intended to prevent authorized users from using the services they have requested. Attacks can happen whether there is a high or low volume of traffic. It's possible to mistake a high-rate traffic attack for a rapid influx of packets into the network. The low-rate traffic, on the other hand, is comparable to typical network traffic. As a result, identifying such attacks is typically challenging. An internet worm that served as a DDoS in the previous decade was able to autonomously find and infect weak devices,

[1]Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[2]Department of Computer Science, (Aided)
Kongunadu Arts and Science College (Autonomous), Coimbatore,
Tamil Nadu, India
* Corresponding Author

infect other vulnerable workstations, and then duplicate itself, flooding the network with a high number of unwelcome messages[6].There are two categories of attacks known as high-rate DDoS attacks and low-rate DDoS attacks. The high-rate flooding attack is also known as a brute force attack, where attackers inundate the targeted cloud server's network capacity with a large volume of malicious requests. This results in a loss of network bandwidth and router processing power, disrupting connectivity. The high-rate assault is categorized as a network or transport-level flooding attack, with examples including Transmission Control Protocol (TCP), User Datagram Protocol (UDP) flood, and Internet Control Message Protocol (ICMP) flood [7]. These attacks aim to render the cloud service unavailable to authorized users by terminating server resources such as memory, disk space, and CPU. They are referred to as application-level attacks and include the Hypertext Transfer Protocol (HTTP) flood attack [8], Domain Name System (DNS) flood attack, and Simple Mail Transfer Protocol (SMTP) flood. Attackers typically identify vulnerabilities in a large number of computers to create attack armies known as botnets to carry out these attacks. The attacker can take control, which is subsequently sent to the cloud server and sent to the many cooperating hosts. One or more cloud servers are the object of the deluge of demands that the cooperative hosts transmit. To conceal its actual origins, the botnet computer system may launch DDoS attacks using an IP spoofing technique. Finding the attacker's actual location is therefore a difficult but crucial task.

Low-rate DDoS Attacks or Semantic attacks, which take advantage of protocol weaknesses, are also known as vulnerability attacks or low-rate attacks. Detecting the lowest-rate DDoS attacks poses a significant challenge compared to high-rate attacks, as these attacks involve a small volume of malicious traffic directed at the target application. Due to their minimal traffic volume and stealthy nature, low-rate DDoS attacks are more intricate and demanding to pinpoint than their high-rate counterparts. These attacks are adept at evading traffic volume-based defense systems, as the attacker utilizes minimal bandwidth to send malicious requests, masking their actions. Instead of halting cloud services altogether, these attacks typically alter the Quality-of-Service (QoS) experienced by authorized users. Four types of low-rate attacks include the shrew attack, RoQ attack, LoRDAS, and EDoS attack.The outline of the paper is as follows,

- An extensive analysis of the many kinds of DDoS attacks, their detection methods, and challenges

- A review of current DDoS attacks on computer networks;

- A systematic taxonomy for identifying anomalous traffic patterns in computer networks

- A thorough analysis of the traditional shortcomings and advantages of DDoS detection methods.

- Lastly, the difficulties with the current system are also covered.

The subsequent sections of the paper are structured as follows: Section 2 delves into the lifespan of a DDoS attack. Section 3 discusses the types and detection of DDoS attacks. Section 4 addresses approaches to deep learning. Section 5 explores relevant works. Section 6 addresses the challenges encountered. Finally, Section 7 encapsulates the paper's conclusion.

1. The life cycle of DDoS attacks

There are four stages to a DDOS assault, including monitoring, detection, prevention, and mitigation. The purpose of monitoring is to gather important data about the network or host. To identify the malicious effort, detection involves examining the network traffic that has been

collected. To safeguard the cloud service and its resources from the development of some apps at multiple locations, prevention is utilized. The attack severity is estimated in the mitigation phase, which then takes specific action to manage its effects. The prevention phase receives the results of the mitigation phase and updates the preventative measures accordingly. Only the detection phase of the four is being thoroughly reviewed in this research.

II. DDOS ATTACK DETECTION

The DDoS attack tries to overload the network, application, computer, and services with traffic so that they are taken offline. A botnet refers to an internet-connected device that controls two or more bots. Botnets can be used for various malicious activities such as DDoS attacks, data theft, spam transmission, and unauthorized access to the target device and its network connection. A botnet may be managed and controlled by the operator using software. Attackers employ botnets of compromised computers to make services unavailable or disconnected from the network[9]. DDoS attack detection techniques are divided into two groups, including application-based and network-based techniques. The user interface layer controls and monitors packets in the network using the application-based approach. the network-based uses several levels of network protocols to track the network traffic. Additionally, signature or anomaly detection may be the foundation of network-based approaches. To find security concerns, a signature-based (or knowledge-based) detection scans network traffic packets for previously recognized attack patterns. Viruses or incomplete packets are two examples. Such techniques can only identify known attacks; thus, the network administrator should constantly add new attack patterns to the detection system. An anomaly-based detection technique, which is based on recent research, finds possible security concerns in a group of packets that exhibit aberrant behavior.

III. DEEP LEARNING

Deep learning, a subset of machine learning, concentrates on deep neural networks characterized by multiple layers. These neural networks are adept at discerning and assimilating intricate data patterns. Deep learning algorithms utilize numerous layers of artificial neural networks to model and execute complex tasks. Each layer of the neural network processes input data and forwards the output to the subsequent layer. Deep learning finds significant utility in applications such as image and speech recognition, natural language processing, and game playing due to its ability to extract complex features from the input data through its deeper layers.

Recently, deep learning (DL) methodologies have been used to identify DDoS attacks more frequently in recent years because of their high detectability. Improved DDoS attack detection and mitigation are made possible by deep learning algorithms. DDoS attacks are nefarious attempts to flood a targeted server or network with incoming traffic to slow down, make users unresponsive, or make the target inaccessible. Deep learning algorithms greatly improve DDoS attack detection systems with their capacity to analyze massive amounts of data, extract pertinent characteristics, adapt to new attack patterns, and work in real time. The versatility and learning abilities of deep learning models make them important weapons in the continuing battle against cyber threats as the environment of DDoS attacks continues to change.

IV. RELATED WORKS

This section provides a thorough review of current detection methods for DDoS attacks, which are enumerated in Table 1.Methods for detecting DDoS attacks using feature extraction from deep belief networks and an LSTM model have been developed. In the hybrid LSTM approach, the prediction error is decreased by combining the Particle Swarm Optimization (PSO) technology with LSTM neural

network weight optimization.This deep belief network technique extracts IP packet characteristics and detects DDoS assaults using the PSO-LSTM model[10].The deep neural network and LSTM used the findings from the three attack detection tests to develop the deep neural network structure that is suitable for the categorization of attacks. With a 99.90–99.97% average accuracy, the Syn Flood, UDP Flood, and UDP-Lag types can discern between "normal" and "abnormal" input[11].The proposed research incorporates various techniques including the Long Short-Term Memory (LSTM) recurrent neural network, an autoencoder and decoder-based deep learning approach, and the gradient descent learning algorithm. To optimize network parameters like weight vectors and bias coefficients effectively, a hybrid optimization technique combining Harris Hawks Optimization (HHO) and Particle Swarm Optimization (PSO) has been suggested [12]. A deep learning-based model utilizing a contractive autoencoder was suggested to find anomalies. Develop a model, train it to understand the typical traffic flow from the compressed form of the input data, and then use a stochastic threshold approach to identify an attack[13].A two-phase deep learning-based DDoS assault detection system was developed based on DL-2P-DDoSADF[14]. The valid traffic was used to train the autoencoder (AE), and the reconstruction error (RE) was used to adjust the threshold value. The effectiveness of the suggested strategy has been confirmed using test data that includes both genuine and attack traffic. Using a trained AE model, the first step involves allowing projected valid traffic to flow across the network. The anticipated attack traffic, however, moves on to the second step to be classified as the sort of attack it is.

A brand-new ML method for intrusion detection that is based on ensembles is introduced[15].Through the use of principal component analysis, mutual information, and correlation analysis, the most pertinent characteristics for intrusion detection are chosen. The detection method employing several ensemble techniques shows that the suggested strategy utilizing the RF methodology performs better than current strategies. This tactic might help enhance the security of networks and computer systems.Constructed a deep network model capable of autonomous feature extraction and applied deep learning principles to enhance the performance of network intrusion detection systems (IDS). This study focuses on analyzing the features associated with time-related intrusions and introduces a novel IDS comprising a recurrent neural network with gated recurrent units (GRU), a multilayer perceptron (MLP), and a softmax module. A unique approach to intrusion detection is proposed, integrating an improved convolutional neural network (CNN) with the adaptive synthetic sampling (ADASYN) algorithm [16]. Initially, the ADASYN technique is employed to balance the sample distribution, preventing the model from being biased towards large samples while neglecting smaller ones. Secondly, the split convolution module (SPCCNN) forms the foundation of the enhanced CNN, enhancing feature diversity and reducing the impact of interchannel information redundancy during model training. Finally, for intrusion detection tasks, an AS-CNN model incorporating ADASYN and SPC-CNN is utilized.

An ensemble learning-based decision tree-recursive feature elimination (DT-RFE)-based information extraction system[17]. To choose features and minimize the feature dimension, first suggest a data processing approach using the DT-RFE. To improve resource efficiency and decrease time complexity, the approach removes duplicate and independent data within the dataset. Recursive Feature Elimination (RFE) and Decision Tree (DT) techniques are combined to create the Stacking ensemble learning algorithm.The lightweight deep learning DDoS detection system utilizing the characteristics of convolutional neural networks (CNNs) called LUCID[18]divides traffic flows into two categories: malicious and benign. The four main

areas contributed to the presented detection method: (1) Introducing a novel approach using a CNN for efficient detection of DDoS traffic with minimal processing overhead; (2) Implementing a preprocessing mechanism that is independent of the dataset to generate traffic observations for online attack detection; (3) Conducting activation analysis to provide insights into DDoS classification within the LUCID (Lightweight, Usable CNN in DDoS Detection) framework; and (4) Empirically validating the proposed solution on a hardware platform with limited resources.The emphasis is on concentrating autoencoder-based deep learning techniques and technologies for network flow models in order to classify network traffic [19]. Additionally, a model relying on deep neural networks has been utilized to enhance the classification performance. The proposed model's primary goal is to precisely classify malicious network traffic from packets by using a hybrid model method. The model's autoencoder layer picks up the network flows' representation. The deep neural network model in the second layer looks for certain kinds of harmful activities.

Proposing a tuned vector convolutional deep neural network (TVCDNN) involves optimizing the deep neural network's topology and parameters using binary and real cumulative incarnation (CuI), respectively [20]. The CuI, a genetic-based optimization approach, maximizes the tuning process by utilizing values derived from best-fit parents. Using benchmark network traffic statistics that are accessible to the public, the TVCDNN is evaluated and contrasted with other classifiers and optimization methods already in use.A refined system that can identify DNS-based DOS attacks, which make use of DNS answers to initiate their attacks, is suggested[21]. An adjustable threshold and improved metaheuristic optimization algorithms served as the foundation for the creation of the suggested mechanism. There are four steps and two models in this process. "Proactive Feature Selection" is the name of the first model, while "Evolving Dynamic Fuzzy Clustering" is the name of the second. The preprocessing, feature selection, detection, and augmentation stages are the four phases of the suggested method.

The Improved Salp Swarm Algorithm (ISSA) is implemented for automatic feature selection on binary and multiclass subsets, each processed independently [22]. Following feature selection, the SMOTE–Tomek class balancing approach is employed, utilizing a minimum of four different machine learning (ML) classifiers for binary and multiclass classification. This addresses the challenges of feature selection and class balancing, resulting in the development of an enhanced and more effective NIDPS.

Table 1 : Related works

Author name (s)	Methods	Purpose	Merits	Demerits	Datasets	Measures
A. Thangasamy et al. (2023) [10]	PSO+LSTM	Feature extraction and weight optimization	Reduce the computation time and error	Premature convergence	NSL-KDD	Recall, F-Measure, Precision.
T. Khempetch et al. (2021) [11]	DNN + LSTM	Hyperparameter tuning	High detection rate	Limited datasets	CICDDoS2019	Accuracy Precision Recall F-Measure
S. Sumathi et al. (2022) [12]	HHO-PSO-DLNN	Feature selection and hyperparameters	High detection rate	Static approaches	NSL-KDD	Accuracy Precision Sensitivity Specificity F1 score
S. Aktar et 8yrfdc al. (2023) [13]	autoencoder	Parameter optimization	High accuracy	Possible false alarms	CICIDS2017, NSL-KDD, and CIC-DDoS2019.	Precision-Recall F1-Score Accuracy (%)
M. Mittal, et al. (2023) [14]	DL-2P-DDoSADF	Learning process	High detection accuracy	Low convergence rate	CICDDoS2019 and DDoS-AT-2022	Precision, Recall, F1-Score, and Accuracy
M. A. Hossain et al. (2023)[15]	GRU	Feature selection	Low false positive rates (FPR)	Lacks in optimization	NSL-KDD	Precision, Recall, F1-Score, Accuracy, FPR, Detection Rate (DR)
C. Xu et al. (2018) [16]	AS-CNN	An improve the learning and recognition ability	High computational cost	Ignore the small samples	NSL-KDD	ACC, FAR, and DR
W. Lian et al. (2020) [17]	DT-RFE	Feature Elimination	Low computation time	Lacks inaccuracy	NSL-KDD	Accuracy
R. Doriguzzi-Corin et al. (2020) [18]	LUCID and NTT	Novel preprocessing method	hyperparameter optimization	High computational cost	ISCX2012, CIC2017, and CSECIC2018	Accuracy FPR, Precision PPV, TPR, and F1 Score (F1)
F. O. Catak et al. (2019) [19]	Autoencoder-based deep neural network	Classification	High classification accuracy	Lacks in timestamps	KDDCUP99	Accuracy Precision-Recall and F1-Score
N. B. Amma et al. (2022) [20]	TVCDNN	Parameter optimization	Finding more appropriate parameter	Convergences rate is low	KDD Cup and NSL KDD	Accuracy Precision Error rate
S. Manickam et al. (2022) [21]	EDFC	Feature selection	Low computational cost	Low accuracy	CICDDoS2019	DR FPR
A. Alabrah et al. (2023)[22]	ISSA	Feature selection	High accuracy	Low convergence rate	UNSW-NB15	Accuracy Precision Recall F1-Score
R. Abu Bakar et al. (2022) [23]	ML approaches	Feature extractions	High processing	Stuck inaccuracy	CICIDS2017, CSE-CIC-IDS2018 customized dataset	Accuracy Precision Recall F1-Score
H. Peng et al. (2023) [24]	CNNs +BiLSTMs	Spatial and temporal features extraction	Superior detection accuracy	more computational resources	NSL-KDD, UNSW-NB15, and CIC-IDS2017	accuracy, recall, precision, and F1 score

An intelligent agent system that uses autonomous feature extraction and selection to identify DDoS attacks [23]. In this system, the created approach also constructed an agent-based mechanism that integrates sequential feature selection and machine learning techniques. When the system dynamically identified DDoS attack traffic, the system learning phase picked the best attributes and rebuilt the DDoS detector agent. Introducing a novel neural information detection system (NIDS) known as CBF-IDS, which uses the focal loss function to integrate convolutional neural networks (CNNs) with bidirectional long short-term memory networks (BiLSTMs) [24]. Spatial and temporal information may be retrieved from network data by using CBF-IDS. Additionally, CBF-IDS uses the focal loss function to provide additional weight to minority class samples during model training, reducing the negative effects of class imbalance on model performance.

V. CHALLENGES

Despite the potential advantages of applying advanced machine learning methods, detecting DDoS attacks using deep learning approaches faces various difficulties. The following are some of the main difficulties in DDoS attack detection using deep learning:

- Imbalanced dataset: Datasets for DDoS attacks are sometimes quite unbalanced, with a large percentage of cases representing regular traffic and a disproportionately small percentage representing attack instances. Deep learning algorithms need balanced datasets to work well, and biased models might result from imbalanced data.

- Feature engineering:The effectiveness of deep learning models is greatly influenced by the quality and relevance of the input data. To identify significant patterns in network traffic data, feature engineering is essential. Designing effective features for DDoS attack detection is difficult, especially given how frequently DDoS attacks change.

- Dynamic behavior:Because networks are dynamic and ever-evolving, models developed for one network may not generalize effectively to another. It can be difficult to adjust deep learning models to various network setups and behaviors, especially in real-time settings.

- Real-Time: DDoS attacks may start very quickly and overwhelm a network in an instant of minutes. Due to their computational expense, deep learning models, particularly sophisticated ones, may not be appropriate for real-time detection. For prompt detection and reaction, effective implementation and optimization are required.

- Interpretability: It can be challenging to comprehend the logic behind the predictions made by deep learning models, especially deep neural networks, which are sometimes referred to as "black boxes." Understanding why a particular traffic instance was labeled as an attack or normal in the context of DDoS attack detection might be critical for network managers.

VI. CONCLUSION

An extensive examination of deep learning-based methods for recognizing different kinds of DDoS attacks has been presented in this work. This survey helps the authors identify various DDoS attacks and offers workable fixes to prevent network outages and ensure successful transmission. These surveys aid in the analysis of the benefits and drawbacks of various attacks and their remedies. We anticipate that this clever strategy, which offers a full suite of estimating tools for detecting different kinds of DDoS attacks, will help with future solutions. Finally, we have brought attention to ongoing concerns that remain a threat and have identified various topics that warrant further exploration in future research.

REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176-8186, 2021.

[2] I. Ortet Lopes, D. Zou, F. A. Ruambo, S. Akbar, and B. Yuan, "Towards effective detection of recent DDoS attacks: A deep learning approach," Security and Communication Networks, vol. 2021, pp. 1-14, 2021.

[3] [Online]. Available: https://www.bbc.com/news/technology-53093611.

[4] [Online] Available: https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

[5] https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021 (accessed.

[6] M. Nooribakhsh and M. Mollamotalebi, "A review on statistical approaches for anomaly detection in DDoS attacks," Information Security Journal: A Global Perspective, vol. 29, no. 3, pp. 118-133, 2020.

[7] O. A. Osanaiye and M. Dlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment," in IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON), 2015: IEEE, pp. 1-6.

[8] M. Idhammad, K. Afdel, and M. Belouch, "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest," Security and Communication Networks, vol. 2018, 2018.

[9] H. Beitollahi, D. M. Sharif, and M. Fazeli, "Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function," IEEE Access, vol. 10, pp. 63844-63854, 2022.

[10] A. Thangasamy, B. Sundan, and L. Govindaraj, "A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques," Computer Systems Science & Engineering, vol. 45, no. 3, 2023.

[11] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," IAES International Journal of Artificial Intelligence, vol. 10, no. 2, p. 382, 2021.

[12] S. Sumathi, R. Rajesh, and S. Lim, "Recurrent and deep learning neural network models for DDoS attack detection," Journal of Sensors, vol. 2022, 2022.

[13] S. Aktar and A. Y. Nur, "Towards DDoS attack detection using deep learning approach," Computers & Security, vol. 129, p. 103251, 2023.

[14] M. Mittal, K. Kumar, and S. Behal, "DL-2P-DDoSADF: Deep learning-based two-phase DDoS attack detection framework," Journal of Information Security and Applications, vol. 78, p. 103609, 2023.

[15] M. A. Hossain and M. S. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," Array, vol. 19, p. 100306, 2023.

[16] Z. Hu, L. Wang, L. Qi, Y. Li, and W. Yang, "A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network," IEEE Access, vol. 8, pp. 195741-195751, 2020.

[17] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," Mathematical Problems in Engineering, vol. 2020, pp. 1-15, 2020.

[18] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "LUCID: A practical, lightweight deep learning solution for DDoS attack detection," IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 876-889, 2020.

[19] F. O. Catak and A. F. Mustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," Journal of Intelligent & Fuzzy Systems, vol. 37, no. 3, pp. 3969-3979, 2019.

[20] N. B. Amma and S. Selvakumar, "Optimization of vector convolutional deep neural network using binary real cumulative incarnation for detection of distributed denial of service attacks," Neural Computing and Applications, pp. 1-14, 2022.

[21] S. Manickam, R. Rahef Nuiaa, A. Hakem Alsaeedi, Z. A. A. Alyasseri, M. A. Mohammed, and M. M. Jaber, "An enhanced mechanism for detection of Domain Name System-based distributed reflection denial of service attacks depending on modified metaheuristic algorithms and adaptive thresholding techniques," IET Networks, vol. 11, no. 5, pp. 169-181, 2022.

[22] A. Alabrah, "An Efficient NIDPS with Improved Salp Swarm Feature Optimization Method," Applied Sciences, vol. 13, no. 12, p. 7002, 2023.

[23] R. Abu Bakar, X. Huang, M. S. Javed, S. Hussain, and M. F. Majeed, "An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection," Sensors, vol. 23, no. 6, p. 3333, 2023.

[24] H. Peng, C. Wu, and Y. Xiao, "CBF-IDS: Addressing Class Imbalance Using CNN-BiLSTM with Focal Loss in Network Intrusion Detection System," Applied Sciences, vol. 13, no. 21, p. 11629, 2023.